febelfin

# Don’t be fooled by a ‘phish’

Bankzaken regelen, boodschappen doen, vakanties boeken...alles gebeurt meer en meer online. Dit betekent jammer genoeg ook dat de criminaliteit zich verplaatst naar de digitale wereld. Het  is  voor fraudeurs dé plek geworden om mensen financieel op te lichten.

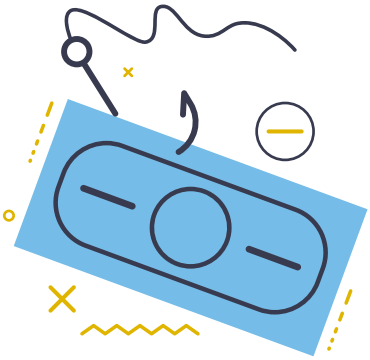
In 2022 hebben cybercriminelen massaal veel phishingberichten uitgestuurd en zich daarbij voorgedaan als vertrouwde organisaties, zoals banken, nutsbedrijven en overheidsdiensten. Ongeacht leeftijd, opleidingsniveau, taal... iedereen ligt in het vizier van cybercriminelen, helaas ook jongeren. Voortdurende waakzaamheid blijft dus de boodschap.

Hoe evolueert online fraude en wat zijn de meest actuele fraudevormen? Zijn 'phishing' en 'geldezels' voldoende gekend? Waar legt de sector zijn focus? Lees er alles over in deze nieuwe storytelling, boordevol nieuwe onderzoekscijfers[1].

## WAT IS PHISHING?

Het is een vorm van fraude waarbij criminelen naar de persoonlijke bankcodes van hun potentiële slachtoffers hengelen door zich voor te doen als een gekende of vertrouwde organisatie.

# MEER PHISHINGBERICHTEN IN 2022, DUS MEER BUIT



**€ 39,8 miljoen** buit in 2022

In 2022 werd er in totaal 39,8 miljoen euro buit gemaakt naar aanleiding van phishing, een stijging in vergelijking met vorig jaar (2021: 25 miljoen euro). Dit is vooral te wijten aan de **enorme stijging** van het aantal **uitgestuurde phishingberichten**.

De omvang van al deze phishingpogingen wordt bevestigd door de resultaten van de Febelfin studie in samenwerking met het onderzoeksbureau Indiville. Volgens deze studie heeft 69% van de Belgen de afgelopen 6 maanden[2] minstens één phishingbericht ontvangen.

Ook de cijfers van het Centrum voor Cybersecurity België bevestigen deze stijging: Belgische internetgebruikers stuurden in 2022 maar liefst 6 miljoen verdachte berichten door naar het e-mailadres verdacht@safeonweb.be, dat zijn 1,5 miljoen berichten meer dan in 2021.

[1] IndiVille onderzoek, 3-20 maart 2023, op een representatief staal van de Belgische bevolking n: 2117 NL/FR enquêtes, leeftijd 16-79. Maximale margefout: 2,1%.

[2] Meer bepaald de laatste 3 maanden van 2022 en de eerste 3 maanden van 2023.

# Oplichters ‘vissen’ naar gegevens, maar hoe ze dat doen varieert.

Phishing is geen nieuw fenomeen.
Er is een **constante in het phishingverhaal**: De fraudeurs hengelen naar (bank)gegevens via verschillende kanalen zoals e-mail, telefoon, brief, sms, sociale media of WhatsApp. Ze proberen mensen financieel op te lichten door zich voor te doen als betrouwbare organisaties of instellingen (banken, overheidsdiensten, nutsbedrijven...). Het verzonden bericht bevat een link naar een valse website, waar het slachtoffer wordt gevraagd om persoonlijke bankcodes in te voeren. Zodra de fraudeurs deze persoonlijke bankcodes in handen krijgen, kunnen ze namens het slachtoffer transacties uitvoeren.

## BANKKAARTPHISHING

Bij bankkaartphishing gaan fraudeurs via e-mail, telefoon of sms vragen om je bankkaart per post naar een bepaald adres te sturen. Tegelijk bezorgen ze je een link naar een valse website, waar je je persoonlijke codes moet ingeven. Zo hebben de fraudeurs in één klap je bankkaart en je persoonlijke codes.

## BANKKAARTPHISHING AAN HUIS

Bij bankkaartphishing aan huis gaat de fraudeur zich voordoen als een bankmedewerker, je opbellen en melden dat er verdachte transacties op je rekening zijn opgemerkt. Hij biedt aan om bij jou thuis langs te komen om de situatie op te lossen. De fraudeur laat je dan bijvoorbeeld inloggen bij jouw online bank. Zo kan die gemakkelijk je persoonlijke code noteren.

Tegenwoordig zijn er ook **variaties** op phishing, namelijk **bankkaartphishing** of bankkaartphishing aan huis.

Cybercriminelen spelen ook in op de actualiteit. Met de **energiecrisis** in 2022 werd de Belgische bevolking overspoeld met frauduleuze berichten die premies of andere vormen van overheidssteun beloofden, gelet op de torenhoge energieprijzen. De cybercriminelen deden hun uiterste best om hun potentiële slachtoffers te verleiden tot klikken, vooral in een periode waarin er veel onzekerheid bestond over de gevolgen van de energiecrisis en de toenemende inflatie.

# ANDERE VAAK VOORKOMENDE FRAUDEVORMEN

In 2021 zagen we een aanzienlijke verschuiving naar andere fraudevormen, zoals beleggingsfraude, factuurfraude, kluisrekeningfraude, hulpvraagfraude... Fraudevormen waarbij het **slachtoffer** wordt **gemanipuleerd en overtuigd om zelf geld over te maken**. In 2022 is het aandeel van deze fraudevormen **stabiel** gebleven, we zagen geen bijzondere toe- of afname hiervan.

## HULPVRAAGFRAUDE

Bij hulpvraagfraude doen fraudeurs zich via e-mail, sms of berichten op social media voor als één van jouw dierbaren. Of omgekeerd: ze schrijven je dierbaren aan in jouw naam. Ze vragen om dringende financiële hulp.

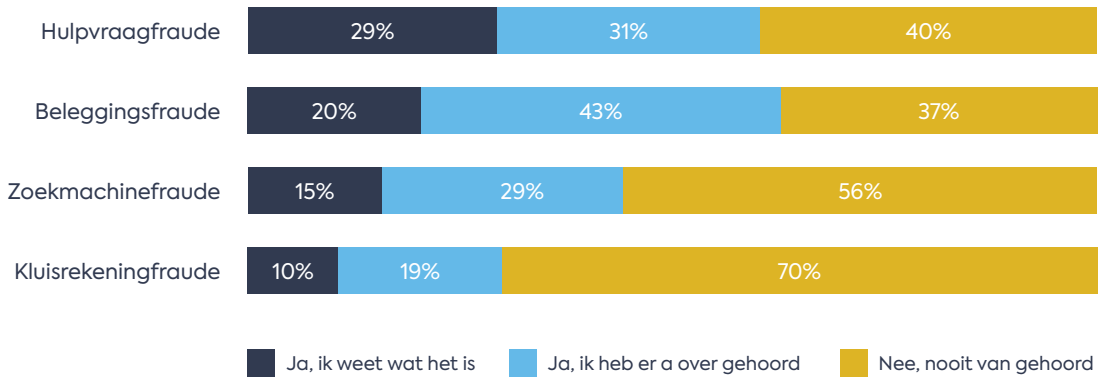
## Belgen niet altijd op de hoogte van actuele fraudevormen.

## BELEGGINGSFRAUDE

Bij beleggingsfraude gaan fraudeurs je een "fantastische" deal (investering) aanbieden die een hoog rendement belooft op te leveren. Die belegging blijkt achteraf niet te bestaan.

Uit de resultaten van de Indiville studie[3] blijkt dat de Belgen hun kennis over de (nieuwe) fraudevormen nog moeten verhogen.

**Weet je wat deze vormen van fraude zijn?**




*Bron: Indiville-studie*

[3] IndiVille onderzoek, 3-20 maart 2023, op een representatief staal van de Belgische bevolking n: 2117 NL/FR enquêtes, leeftijd 16-79. Maximale margefout: 2,1%.

**Hulpvraag-en beleggingsfraude** zijn iets beter bekend bij de bevolking: 60% van de Belgen heeft al van hulpvraagfraude gehoord en 63% van beleggingsfraude. Daarentegen weet minder dan de helft van de Belgen wat **zoekmachinefraude** en **kluisrekeningfraude** inhoudt.

De voorbije jaren heeft Febelfin door middel van verschillende persberichten en beeldmateriaal (posters, stickers, spelboekje...) geprobeerd de bevolking (meer) bewust te maken van de verschillende fraudevormen en geïnformeerd over de risico's en preventieve maatregelen die genomen kunnen worden. Het doel was om de bevolking te helpen fraude beter te herkennen en zichzelf te beschermen tegen allerlei vormen van online oplichting. Het is van groot belang om constant waakzaam te blijven en regelmatig informatie en updates over dit onderwerp te delen, zodat we gezamenlijk kunnen strijden tegen deze fraudevormen en de schadelijke gevolgen ervan kunnen verminderen.

## KLUISREKENINGFRAUDE

Bij kluisrekeningfraude gaan oplichters je eerst (maar niet altijd) een phishingbericht sturen om je persoonlijke bankcodes te verkrijgen. Zo proberen ze toegang te krijgen tot je rekening. Daarna bellen ze je op. Ze doen zich dan voor als een medewerker van je bank en vragen je om geld over te schrijven naar een zogezegd nieuwe, veilige rekening. Deze fraudevorm richt zich vooral op senioren.



*Poster en stickers om senioren te sensibiliseren voor actuele fraudevormen.*

# HEEFT DE BELG DE VOORBIJE JAREN IETS GELEERD OVER PHISHING EN GELDEZELS?

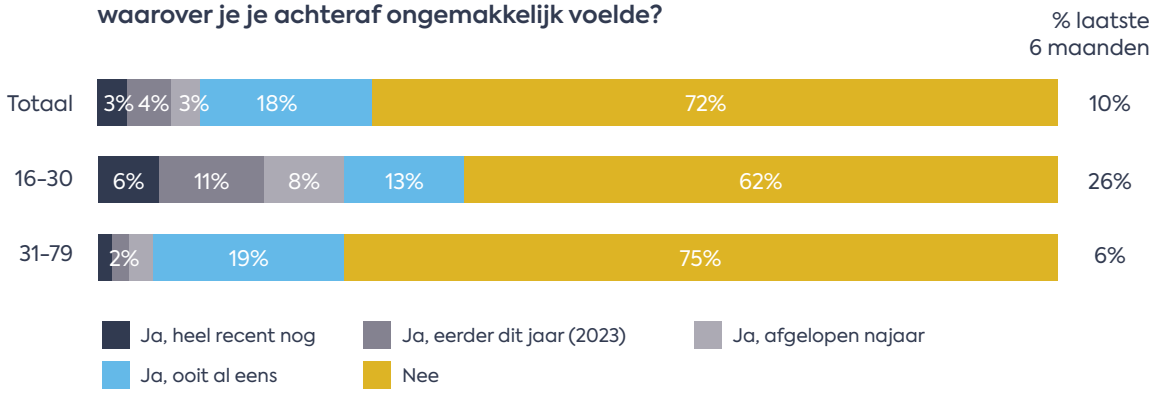
De problematiek van phishing, geldezels en online fraude in het algemeen blijft nog te groot maar uit het Indiville onderzoek blijkt dat de manier waarop de Belg met online fraude omgaat, verbeterd is. Acties van de sector en zijn partners beginnen stilaan hun vruchten af te werpen maar continue voorlichting blijft noodzakelijk, zeker bij jongeren en ook gelet op de toegenomen phishingpogingen. Door de toename in verstuurde phishingberichten, heeft het bewuster gedrag van de Belg, jammer genoeg nog niet tot minder schade geleid.

## PHISHING

### We delen minder financiële informatie en nemen meer actie

10% van de bevolking deelde in 2023 financiële informatie waarover ze zich ongemakkelijk voelden (in 2022 was dit nog 11%). Dit percentage ligt iets hoger bij de leeftijdsgroep van 16-30 jaar (18%), maar het is een verbetering ten opzichte van 2022 (25%).

**Heb jij ooit al financiële gegevens online doorgegeven waarover je je achteraf ongemakkelijk voelde?**

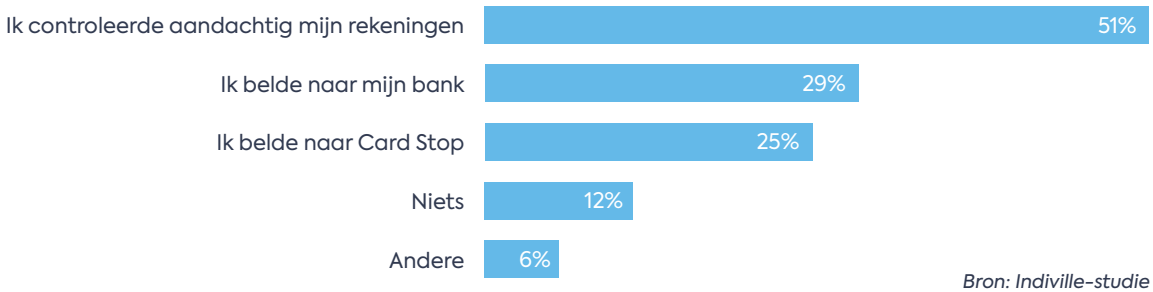



*Bron: Indiville-studie*

Wat ook positief is, is dat **88%** van de ondervraagden **actie ondernam** na het delen van deze informatie. Zoals blijkt uit de grafiek hieronder controleerde 51% van de ondervraagden zijn/haar rekeningen na het delen van financiële informatie. De oudere leeftijdsgroep controleert iets vaker hun rekeningen dan de jongeren (55% versus 44%).

29% van de ondervraagden nam contact op met zijn/haar bank en 25% belde naar Card Stop.

**Wat deed je met dit gevoel?**

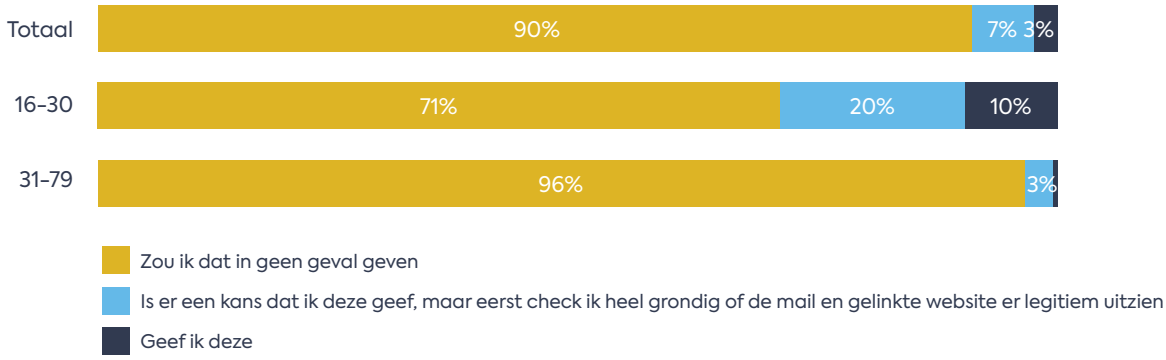



*Bron: Indiville-studie*

## 9 Belgen op 10 zouden in geen enkel geval hun codes aan de bank doorgeven.

Toch is er nog steeds 3% van de bevolking die zonder aarzelen hun bankcodes zou delen als hun bank erom zou vragen (in 2022 was dit nog 5%). Vooral **jongeren** blijven **kwetsbaarder**, waarbij 10% in de leeftijdsgroep van 16-30 jaar gemakkelijker hun bankcodes deelt dan andere leeftijdsgroepen. Hoewel dit percentage nog steeds veel te hoog is, is er wel een **verbetering ten opzichte van 2022**, toen het percentage 13% bedroeg. Het is positief om te zien dat er een verbetering is ten opzichte van het voorgaande jaar wat betreft het delen van bankcodes. Dit betekent dat er **meer bewustzijn** is ontstaan over **de risico's van het delen van persoonlijke bankinformatie**, maar de cijfers tonen ook aan dat sensibilisering noodzakelijk blijft.

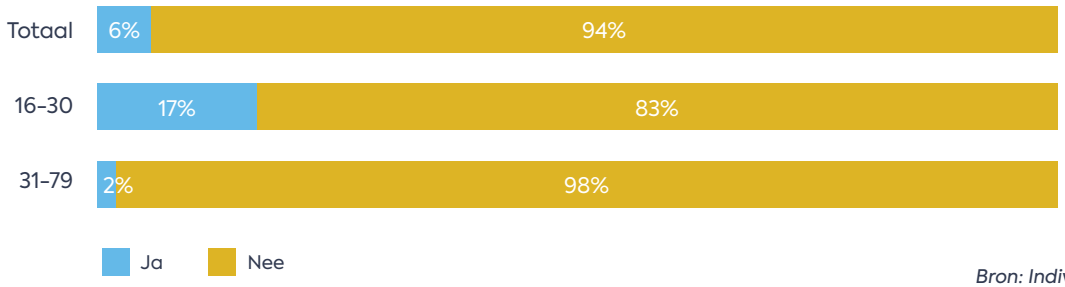
**Als je bank via e-mail, sms, whatsapp, telefoon ... naar mijn bankcodes vraagt ...**




*Bron: Indiville-studie*

Daarnaast kunnen we vaststellen dat **6%** van de bevolking bereid zou zijn hun **bankkaart terug te sturen als de bank daarom zou vragen**. Bij de jongeren tussen 16 en 30 jaar, loopt dit cijfer echter op tot 17%. De bijzondere kwetsbaarheid van jongeren inzake online fraude blijft bijzonder verontrustend.

**Zou je je bankkaart terugsturen als je bank via e-mail, sms, whatsapp, telefoon, brief... hierom vraagt?**



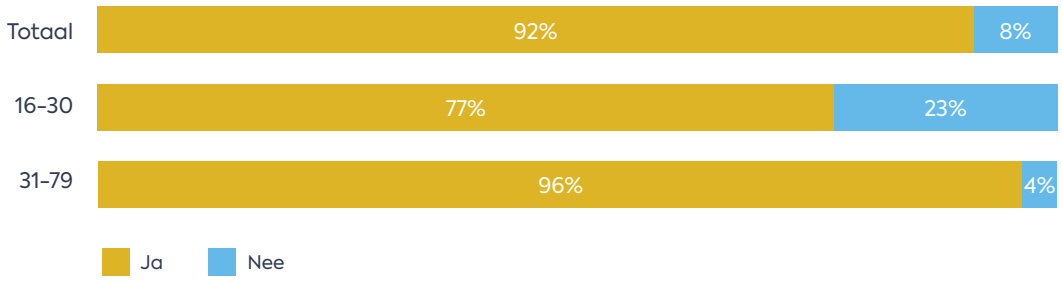

*Bron: Indiville-studie*

## Vooral jongeren weten niet wat 'phishing' is

**8%** van de Belgen heeft **nog nooit gehoord van phishing**. De oudere leeftijdsgroep scoort op dit vlak beter, 4% heeft nog nooit van phishing heeft gehoord, wat een verbetering is ten opzichte van 2022 (7%).

Hoewel er sprake is van een lichte verbetering ten opzichte van 2021 (24%) en 2022 (30%), is het aantal **jongeren** die niet weet wat phishing is, te hoog (**23%**).

**Heb je ooit al gehoord van phishing?**

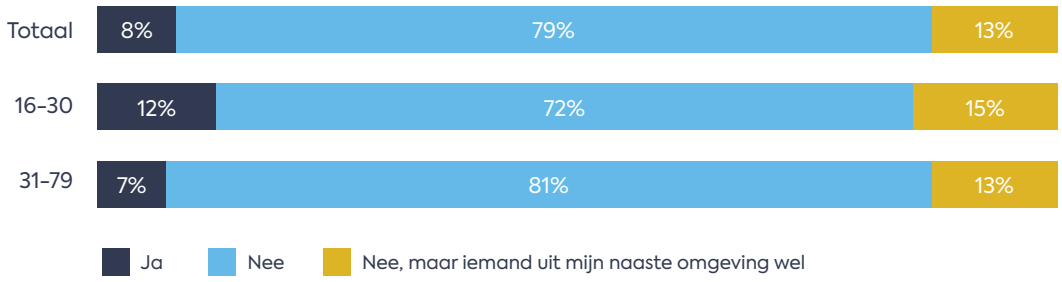



*Bron: Indiville-studie*

## Bijna 1 op 10 Belgen werd ooit slachtoffer van phishing

**8%** van de Belgen geeft aan slachtoffer te zijn geworden van phishing. Bij jongeren ligt dit percentage hoger, namelijk 12%. Ondanks dat jongeren opgroeien met digitale technologie en vaak als 'digital natives' worden gezien, betekent dit jammer genoeg niet dat ze over alle digitale vaardigheden beschikken en goed op de hoogte zijn van online veiligheid. Bovendien behoren zij ook tot de bevolkingsgroep die het meest aangeeft iemand te kennen die al slachtoffer is geworden van phishing, namelijk 15%.

**Ben je al slachtoffer geworden van phishing?**




*Bron: Indiville-studie*

Deze bevindingen benadrukken het belang van gerichte educatie en bewustwording over online veiligheid, specifiek gericht op jongeren. Het is cruciaal om hen de nodige kennis en vaardigheden bij te brengen om zichzelf te beschermen tegen phishingaanvallen en andere vormen van online fraude.

## Als we ons laten vangen, dan weten we niet wat we moeten doen

Slechts 62% van de Belgen die slachtoffer werden van phishing wisten **welke stappen** ze moesten ondernemen.

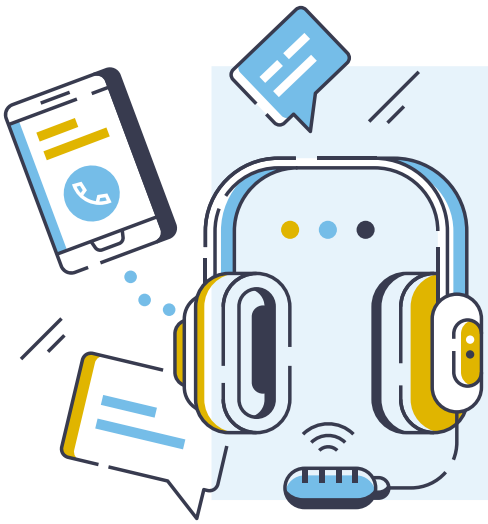
**Wist je welke stappen je moest ondernemen of waar je terecht kon voor hulp?**


*Bron: Indiville-studie*

CARD STOP 078 170 170 24/24

### SLACHTOFFER? VOLG DEZE STAPPEN:

- Bel Card Stop op 078 170 170 om je bankkaart te blokkeren.
- Neem zo snel mogelijk contact op met je bank om ook je bankapplicatie te blokkeren. Alle contactgegevens van de banken in geval van fraude zijn op de website van Card Stop vermeld.
- Dien een klacht in bij de politie.



### WIST JE DAT...

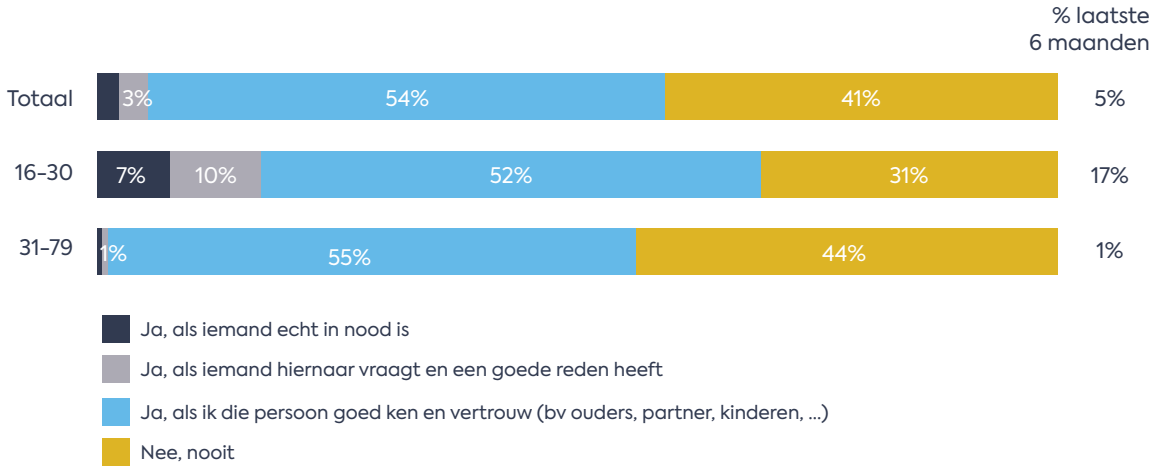
banken permanent beschikbaar zijn in geval van online fraude? Cybercriminelen kunnen op elk moment een misdrijf plegen, ook na de kantooruren of in het weekend. Het is daarom belangrijk dat banken een continue klantendienst aanbieden in geval van online fraude. De banken zijn 24/7 bereikbaar via speciale fraudenummers.

# GELDEZELS

## Je bankkaart en pincode uitlenen is geen goed idee

Je bankkaart en je pincode zijn strikt persoonlijk en zeker niet bedoeld om gedeeld te worden met onbekenden. Toch zou nog **5%** van de Belgische bevolking hun bankkaart met pincode geven aan iemand die ze niet kennen, in ruil voor geld. En opnieuw zijn de 16-30 jarigen kwetsbaarder dan de oudere leeftijdsgroep: **17% van de jongeren zou dat doen**, wat de cijfers van 2022 bevestigt.

**Zou jij je bankkaart en pincode afgeven aan iemand anders?**




*Bron: Indiville-studie*

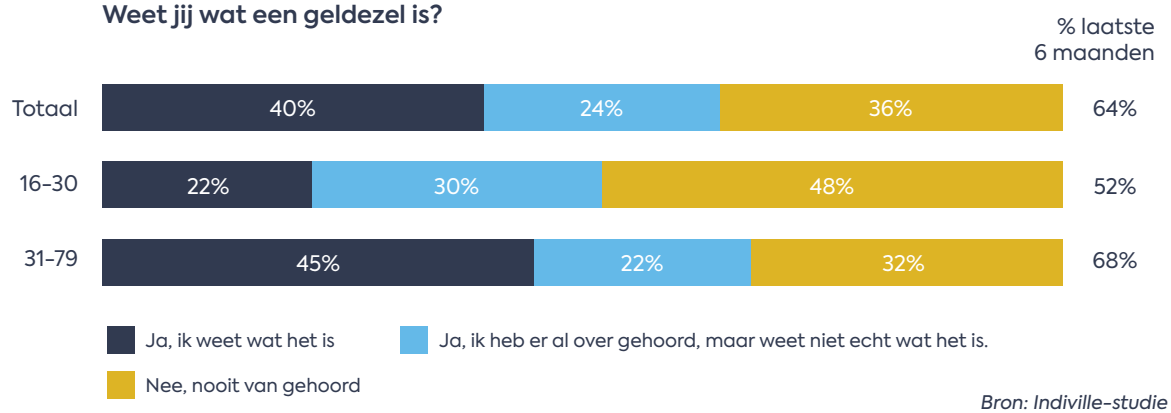
## Verwoest je leven niet door geldezel te worden

Het uitlenen van je bankkaart aan iemand in ruil voor geld, oftewel het worden van een geldezel, kan een zware impact hebben op je leven. Hoewel 40% van de bevolking bekend is met het concept 'geldezel', is dit percentage aanzienlijk lager bij jongeren. Slechts 22% van hen kan een duidelijke uitleg geven over wat een geldezel is. Dit gebrek aan kennis maakt dat jongeren zich ook onvoldoende bewust zijn van de gevaren die hiermee gepaard gaan en het feit dat het strafbaar is.

## WAT IS EEN GELDEZEL?

Een geldezel is iemand die zijn bankrekening en/of bankkaart en pincode laat gebruiken door criminelen om crimineel geld wit te wassen. Daardoor kan de crimineel misdaadgeld op de bankrekening van de geldezel storten om het vervolgens af te halen (met de bankkaart en de pincode van de geldezel) of door te storten naar andere rekeningen. Zo blijven de oplichters buiten schot.

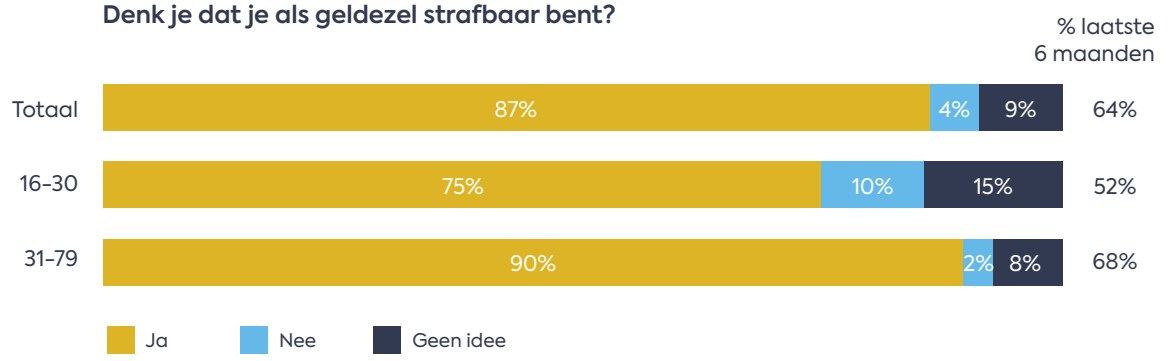
**Weet jij wat een geldezel is?**




*Bron: Indiville-studie*

Opvallend is dat 10% van de jongeren zelfs overtuigd is dat het niet strafbaar is om een geldezel te zijn. Dit maakt hen kwetsbaar voor misleiding en mogelijke juridische gevolgen. Van de 7% van de jongeren die ooit gevraagd is om een geldezel te worden, zou 3 op 4 daadwerkelijk op dit verzoek zijn ingegaan.

**Denk je dat je als geldezel strafbaar bent?**




*Bron: Indiville-studie*

Het is dus van groot belang om jongeren te blijven informeren over het fenomeen van geldezels en de risico's en strafbaarheid ervan.

# ONLINE VEILIGHEID BLIJFT TOPPRIORITEIT VOOR DE BANKEN

Voor de banksector is het essentieel om de veiligheid van online bankieren te waarborgen en fraudepraktijken tegen te gaan. Met **partnerschappen, innovatieve projecten, intensieve monitoring, educatieve programma's en sensibilisering**, streeft de banksector ernaar om fraudepogingen zoveel mogelijk tegen te houden, de kennis over veilig bankieren en verschillende vormen van online fraude te vergroten om zo de bevolking beter beschermen tegen de gevaren van cybercriminaliteit.

## INTENSIEVE MONITORING EN INNOVATIEVE PROJECTEN HELPEN

### Overgrote deel van de frauduleuze overschrijvingen via phishing wordt gedetecteerd, geblokkeerd of teruggevorderd

Banken nemen vele maatregelen om veilige banksystemen te waarborgen en klanten in staat te stellen hun transacties veilig uit te voeren. Ze **monitoren voortdurend de transacties** om verdachte patronen op te sporen. Wanneer de bank een verdachte betalingsopdracht detecteert, wordt deze niet onmiddellijk verwerkt. Er worden eerst aanvullende controles uitgevoerd.

In bepaalde gevallen kan de bank rechtstreeks contact opnemen met de klant om de betalingsopdracht te verifiëren. Dankzij intensieve monitoring kunnen ook veel schades worden voorkomen:

**Ongeveer 75% van alle frauduleuze overschrijvingen n.a.v. phishing werd gedetecteerd en geblokkeerd of teruggevorderd.**

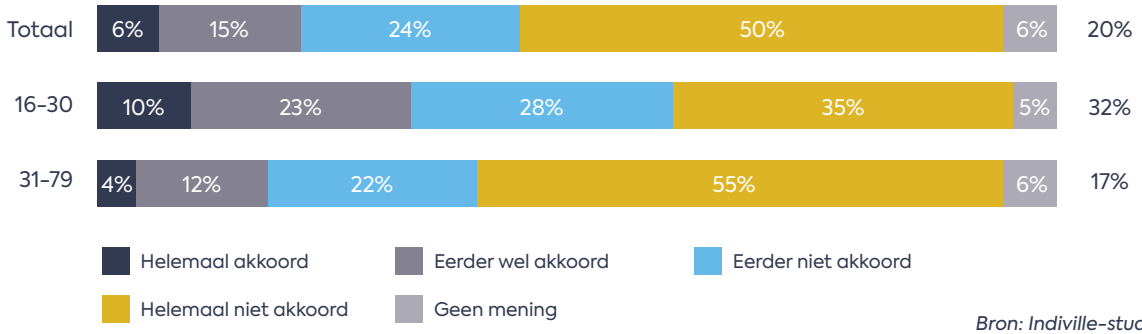
### Authenticatie bij online betalingen

Banken hebben sinds een tiental jaar diverse systemen geïmplementeerd om transacties veilig te laten verlopen bij online en mobiel bankieren, zoals de **sterke klantauthenticatie**. Consumenten worden via SCA (Strong Customer Authentication) extra beschermd doordat ze een extra stap moeten zetten om hun identiteit te bevestigen bij online aankopen of het ondertekenen van betalingen. Deze maatregel is bedoeld om fraude te voorkomen en klanten te beschermen tegen frauduleuze transacties.

Bij deze vorm van authenticatie dient de klant zich te identificeren aan de hand van twee of meer factoren die worden aangemerkt als kennis (iets wat alleen de gebruiker weet), bezit (iets wat alleen de gebruiker heeft) en inherente eigenschap (iets wat de gebruiker is). Meestal gebruik je één van deze factoren, vaak een wachtwoord, om te bewijzen wie je bent, maar voor internet- en mobiel bankieren is het verplicht om er twee of meer te gebruiken.

Positief is dat **steeds minder Belgen (20%) die veiligheidsstappen, als overbodig beschouwen**. Dit is een verbetering ten opzichte van de voorgaande jaren: in 2022 was 26% van de Belgen van mening dat veiligheidsstappen bij online aankopen overbodig waren, terwijl dat percentage in 2021 nog op 33% lag.

**Ik vind het overbodig om verschillende stappen te moeten doorlopen bij online aankopen**




*Bron: Indiville-studie*

Vooral bij jongeren lijkt er nog een zekere nonchalance te heersen op dit gebied, waarbij 32% van de leeftijdsgroep van 16-30 jaar veiligheidsstappen als een hindernis beschouwt (tegen 38% het jaar ervoor). Gelukkig is er bij de jongeren ook sprake van een positieve ontwikkeling, wat aantoont dat de sector moeten blijven uitleggen waarom deze ingebouwde veiligheid in het belang is van de klant.

## Mule Stop proces

Een ander initiatief in de strijd tegen online fraude is het **"mule stop proces"** dat in 2020 werd geïntroduceerd. Dit proces stelt de **bank van het slachtoffer in staat om de bank van de geldezel te verzoeken het overgemaakte fraudebedrag te blokkeren**. Hierdoor kunnen banken snel handelen en financiële schade beperken wanneer er sprake is van geldezels die betrokken zijn bij frauduleuze transacties.

## IBAN-naamcontrole

Daarnaast werkt de banksector aan de implementatie van een **IBAN-naamcontrole** voor digitale overschrijvingen. Deze controle is gericht op het tegengaan van specifieke vormen van fraude, met name factuurfraude. Bij het invoeren van een overschrijvingsopdracht controleert de bank of het rekeningnummer (IBAN) en de naam van de begunstigde overeenkomen. Als er een mismatch wordt gedetecteerd, zal de bank de consument informeren voordat de overschrijving wordt uitgevoerd. De consument kan dan zelf beslissen of hij of zij het overschrijvingsverzoek bevestigt of niet. Deze IBAN-naamcontrole biedt dan ook een extra veiligheidsmaatregel.

# PARTNERSHIPS MET STAKEHOLDERS OVER ALLE SECTOREN HEEN

De financiële sector erkent het belang van nauwe en continue samenwerking met de **telecomsector** en **andere betrokken stakeholders** om de veiligheid van hun klanten te waarborgen. Een indrukwekkend voorbeeld van deze samenwerking is het effectief tegenhouden van **spoofing**. Dankzij deze inspanningen zijn er al ongeveer 100.000 banktelefoonnummers geblokkeerd, waardoor ze niet langer door fraudeurs kunnen worden gebruikt voor spoofing.

Een ander uitstekend voorbeeld van een partnerschap is de samenwerking tussen de Belgische internetproviders, het Centrum voor Cybersecurity België en Febelfin. Gezamenlijk hebben ze een procedure en systeem ontwikkeld, het Belgium Anti-Phishing Shield, dat internetgebruikers waarschuwt voor onveilige websites. Dankzij de samenwerking met de bevolking werden in 2022 maar liefst 14 miljoen kliks naar verdachte websites vermeden, dat zijn ongeveer 25 waarschuwingen naar internetgebruikers per minuut[4].

Dankzij deze strategische samenwerkingen wordt er een sterke verdedigingslinie opgebouwd tegen frauduleuze telefoonnummers en onveilige websites. De politie en justitie staan in voor de opsporing, aanhouding en vervolging van de criminelen, wat voor cyberfraude bijzonder complex en omvangrijk is. Een optimalisering van de samenwerking en organisatie met politie en justitie lijkt aangewezen. Door gezamenlijk op te treden bouwen we samen aan een veiligere digitale omgeving voor de bevolking en dragen we bij aan de algemene strijd tegen cybercriminaliteit.

Bij **spoofing** kan een oplichter op jouw telefoonscherm niet zijn/haar telefoonnummer maar een ander telefoonnummer laten verschijnen.

**Smishing**: phishing via SMS.

[4] 14 miljoen kliks naar verdachte websites vermeden dankzij uniek Anti-Phishing Shield | Centrum voor Cybersecurity België (belgium.be)

# SENSIBILISERING

## Modules om zich te wapenen tegen phishing

Febelfin steunt initiatieven van partners zoals de Belgian Cyber Security Coalition en het Centrum voor Cybersecurity België die een reeks online opleidingen hebben gelanceerd met de titel "Surfen zonder zorgen". Een van de modules genaamd "Kijk waar je naartoe gaat" is nu beschikbaar op de website van Safeonweb. De module bevat informatieve video's die tips geven om frauduleuze links te herkennen. Aan het einde van de module kan je je (opgedane) kennis ook testen via een vragenlijst.

Bovendien zal Febelfin in 2023 opnieuw samenwerken met het Centrum voor Cybersecurity Belgium en de Cybersecurity Coalition aan een grootschalige phishing-campagne.


## Op maat van jongeren

Jongeren beschermen tegen cybercriminaliteit vormt één van de prioriteiten van de banksector. Febelfin erkent het belang om aanwezig te zijn op alle kanalen die door de jongere generatie wordt gebruikt om informatie te verkrijgen, zoals sociale media (Youtube, TikTok, ...) en een dedicated website 'mijngeldenik.be'. Het is onze gedeelde verantwoordelijkheid om ervoor te zorgen dat jongeren toegang hebben tot de juiste en objectieve informatie om hen bewust te maken van de valkuilen en risico's van online fraude, zoals bijvoorbeeld van 'finfluencers'.

mijn geld & ik

## Nieuw: e-learning veilig online bankieren voor de digibegeleider

Febelfin heeft onlangs een nieuwe e-learning ontwikkeld voor digicoaches, d.w.z. vrijwilligers of professionelen die mensen begeleiden bij het ontwikkelen van meer digitale vaardigheden. In de e-learning is er een apart hoofdstuk opgenomen over veilig online bankieren en de verschillende fraudevormen. Febelfin wenst op die manier haar kennis te delen en zoveel mogelijk mensen de kans te bieden om aan de slag te gaan met veilig online bankieren en betalen. De e-learning is gratis en wordt aangeboden in het Frans en het Nederlands.

## Infosessies en webinars

Daarnaast organiseert Febelfin in samenwerking met verschillende partners talrijke fysieke en online **infosessies en webinars** over veilig online bankieren en digitaal betalen, eventueel aangevuld met een toelichting over de verschillende vormen van fraude. We trekken door heel België om zulke sessies te geven en het bewustzijn onder de bevolking te vergroten.

# Gezamenlijke inspanningen en sensibilisering: de sleutel tot het bestrijden van cybercriminaliteit

Alleen door **gezamenlijk de strijd aan te gaan tegen cybercriminaliteit** en **voortdurend** te blijven sensibiliseren, zullen we in staat zijn om cybercriminaliteit terug te dringen. De financiële sector zet zich actief in om fraudepraktijken te bestrijden.

Het is essentieel dat de **banken, de overheid (politie, justitie), bedrijven, de academische wereld en de samenleving als geheel** samenwerken om effectieve maatregelen te nemen om de kennis over online veiligheid en fraude te verbeteren. Door gezamenlijk te leren, te innoveren en informatie uit te wisselen, kunnen we de uitdagingen van de digitale wereld effectief het hoofd bieden. Het is onze gezamenlijke verantwoordelijkheid om ervoor te zorgen dat iedereen, jong en oud, veilig kan navigeren in de digitale wereld. Door te blijven samenwerken en ons bewustzijn te vergroten, kunnen we een **veerkrachtige en veilige digitale omgeving creëren voor de huidige en toekomstige generaties**.


Belgische Federatie van de financiële sector

www.febelfin.be